RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAB2-R05

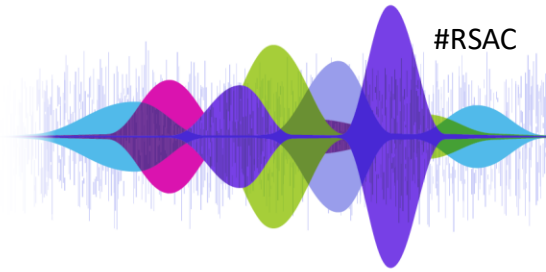
Cybersecurity Game Plan: Crafting Strategies That Win

Rachel Bierner

Co-Founder
Qubric Security
https://www.linkedin.com/in/rkbierner

Cora Quon

Co-Founder
Qubric Security
https://www.linkedin.com/in/cora-quon



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The information in this learning lab is for educational purposes only and should be referenced to fit your organization's specific needs. It does not guarantee security, compliance, or protection against cyber threats.

What is a Cybersecurity Strategy?

What words come to mind when you think of

Cybersecurity Strategy?

Use your phone to scan the QR code and submit your responses.

Cybersecurity Strategy Guidelines

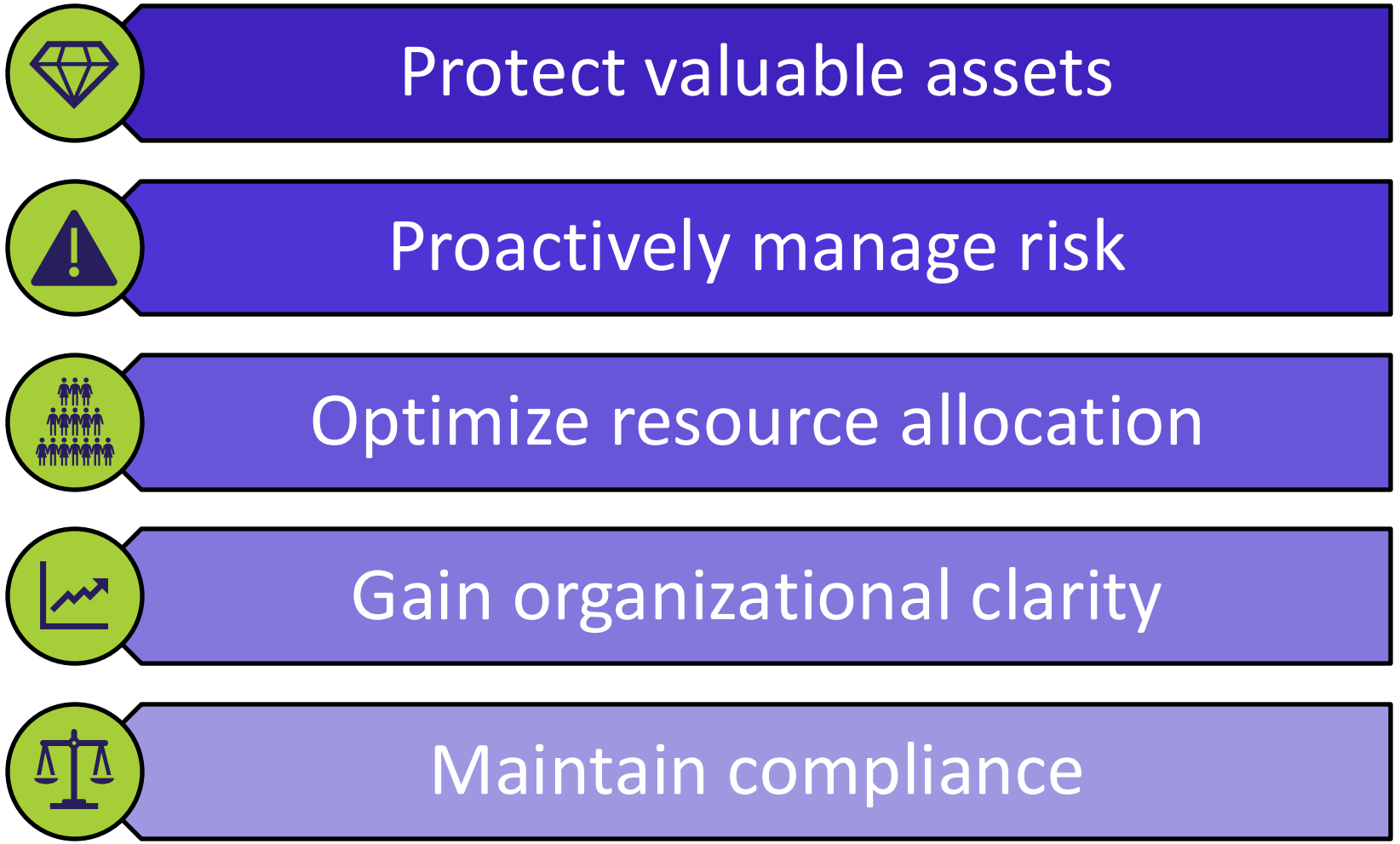
A cyber strategy is:

- Aligned to business goals
- Right-sized
- Proactive
- Long-term
- An ongoing effort

A cyber strategy is not:

- The Vision and Mission statements
- Only a technical roadmap
- A one-time effort
- One-size-fits-all
- Compliance requirements

Benefits of a Cybersecurity Strategy (the Why)



Cybersecurity Strategic Planning Approach

1. DISCOVER	Determine ‘crown jewels’ and what needs to be protected.
2. ASSESS	Assess existing controls against threat environment and identify gaps and opportunities.
3. DEFINE	Identify and establish appropriate program, control, and risk frameworks.
4. DEVELOP	Build strategy with actionable (multi-year) plans and measurable outcomes.
5. ACT	Secure and mobilize resources and execute on plans.
6. MONITOR	Track progress and measure outcomes.
7. IMPROVE	Reassess changes to environment and adjust plans as necessary.

Approach and Components

APPROACH	COMPONENTS – INPUTS	COMPONENTS - OUTPUTS
1. DISCOVER	• Business Objectives • Crown Jewels	• **Vision** • **Mission** • Strategic Business Objectives
2. ASSESS	• Existing Controls • Threat Landscape • Requirements (business, regulatory, etc.)	• **Current State Assessment** • **Risk Assessment**
3. DEFINE	• Vision/Mission • Current State Assessment • Risk Assessment	• **Strategic Cyber Objectives and Goals** • Frameworks
4. DEVELOP	• Cyber Objectives • Frameworks	• **Execution Plan (tasks, outcomes)** • Roadmap
5. ACT	• Leadership Buy-in and Resources	• Outcome Achievement
6. MONITOR	• Execution Plan	• Metrics / Reporting • Progress Updates (against plan)
7. IMPROVE	• Continuous Monitoring	• Strategy/Plan Updates (as needed)

Bolded items are covered in today's Learning Lab in more detail.

Case Study: SecureBank

Objective: Gain hands-on experience working through select key components of a cybersecurity strategy to understand how a comprehensive strategy is structured and developed.

Characteristic	Information
# of Employees	• 1500 (80% employees and 20% contractors) • Information security team made up of CISO and 10 employees • CEO > Chief Information Officer > CISO
Assets Under Management	$5B assets under management with $300MM annual revenue
Business Model	Traditional brick-and-mortar banking with a significant digital presence. Offers online banking, wealth management, loans, and mobile payments.
Technology Footprint	Cloud-based banking services, mobile app for customers, AI-powered fraud detection systems, and third-party integrations with payment providers.
Key Regulatory Requirements	Key requirements include Gramm-Leach-Bliley Act, Federal Financial Institutions Examination Council (FFIEC) cybersecurity guidelines, and PCI DSS (Payment Card Industry Data Security Standard) compliance for payment systems.

Vision & Mission Statements

What is a Vision Statement?

"Provides an inspiring portrait of what it *will look like* and *feel like* to achieve the organization's mission and goals"

- Harvard Business Review

- Your "North Star": aspirational
- In alignment with the business
- A shared *commitment*

What is a Mission Statement?

Articulates ***what*** an organization does - and ***how*** - toward achieving its security goals.

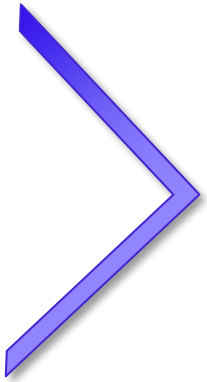
- *What* you do, *who* you serve, and *how* you do it
- A current-day perspective
- A shared *purpose*

Current State Assessment: Overview

Objectives

- Assesses how security programs are currently positioned to protect the organization.
- Identifies opportunities to strengthen the security program and protect from relevant threats.

Inputs:
- Business Requirements
- Regulatory Requirements
- Industry Frameworks
- External Threats
- Existing Controls (People, Processes, and Technology)

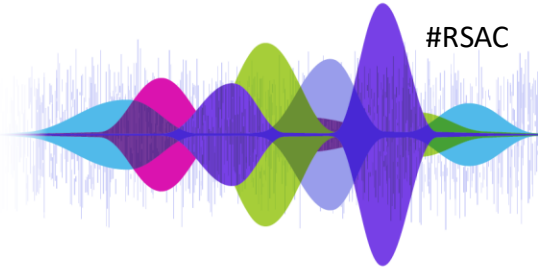


Output:
Identified opportunities and gaps to risk assess and prioritize for execution planning

Current State Assessment: Guidance

- Utilize a well-established cybersecurity framework.
- Organize by cyber domains or topics; cover people, process, policy, and technology.
- Consider the organization's threat surface and risk posture.
- Maintain alignment with business strategy and objectives.

Breakout #1: Current State Assessment



Learning Objective:

- Understand how to identify gaps and opportunities to strengthen an organization's cybersecurity posture based on key inputs.

Instructions:

- Review the inputs provided and identify 2-3 gaps/opportunities to strengthen controls (people, process, policy, and technology) across one cybersecurity domain.

Risk Assessment

Objective

- Assess gaps and opportunities (from Current State Assessment) using a risk management framework to inform action plans.

Guidance

- Articulate risk statements associated with gaps/opportunities.
- Establish a rubric to assess risks consistently. Consider inherent vs. residual vs. treated risk.
- Foster a risk-aware culture – everyone plays a role.
- Risk responses: Avoid, Reduce, Transfer, Accept.
- Ensure right-sized assessment.

Risk Assessment Matrix

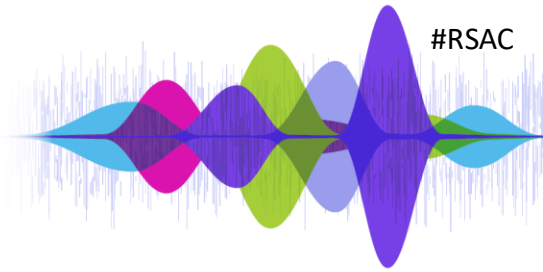
Probability Score (*How likely is this risk to occur given existing controls?*)

Score	Description
1 – Low	Strong controls exist, and no incidents or warning signs suggest this is a realistic concern.
2 – Medium	Some gaps in controls exist, and past incidents or warning signs indicate this could happen.
3 – High	The issue is actively occurring or highly probable due to weak or failing controls.

Impact Score (*What would happen if this risk occurs?*)

Score	Description
1 – Low	Minimal disruption, minor financial loss, or easily contained.
2 – Medium	Some disruption, moderate financial or reputational damage.
3 – High	Severe impact, major financial loss, and/or regulatory consequences.

Note: Organizations should customize the risk matrix based on their needs. For example, quantification of sub-categories - such as assigning percentage intervals to probability and quantifying financial impact - can help drive more consistent risk ratings and provide further context to relative risk.



Breakout #2: Risk Assessment

Learning Objective:

- Determine the relative risk of 2-3 gaps/opportunities identified in the current state assessment.

Instructions:

- Complete a risk-ranking exercise using a qualitative risk matrix based on likelihood and impact.

Target State Planning

Components to planning towards your target state:

Strategic Objectives	*Impactful opportunities to realize or outcomes to achieve.*
Goals	*Near-term, mid-term, and long-term milestones towards each objective.*
Execution Plan	*Prioritized actions needed to achieve stated goals.*

How do we get to our destination?

Strategic Objectives

Clear, specific, and aspirational targets that directionally align with the organization's vision and support the organization's mission.

A strategic objective is:

- An outcome
- SMART: specific, measurable, achievable, realistic, timebound
- A driver of meaningful change
- Dynamic to the landscape

A strategic objective is not:

- A function
- A project
- A metric
- A guiding principle

Setting Goals

Define targets with near-, mid-, and long-term milestones toward achieving your strategic objectives.

Characteristics of strong goals:

- Strategic alignment with buy-in
- Iterative, progressive
- Lead to tangible outputs and outcomes

Guideline for timeframes:

- *Near-term*: within 1 planning/budget cycle
- *Mid-term*: within 2-3 planning/budget cycles
- *Long-term*: 3-5 years out

Execution Planning

A schedule of prioritized and sequenced actions to be taken to achieve strategic objectives.

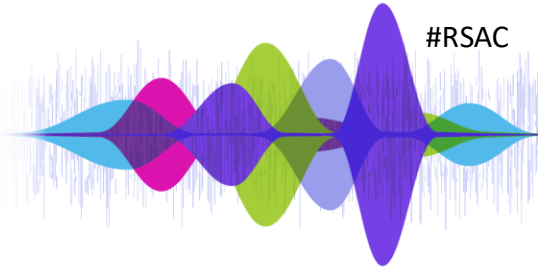
An Execution Plan consists of:

A timeline of actions

Prioritized and sequenced initiatives with clear ownership

Resource specifications (people, time, money)

Breakout #3: Target State Planning



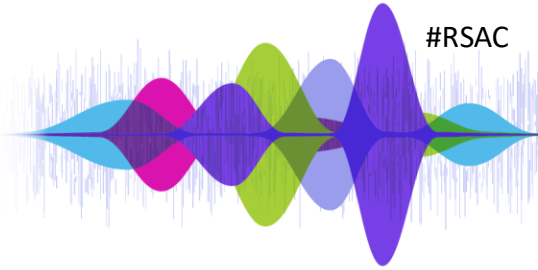
Learning Objective:

- Understand how to define strategic objectives and iterative goals based on the Current State and Risk assessments and aligned to the organization's Vision and Mission.

Instructions:

- Define at least one target state, strategic objective for SecureBank. Decompose the objective to specify goals with near-, mid-, and long-term milestones. Time permitting, define supporting projects with estimated resource needs (S, M, L).

Apply What You Have Learned Today



- **Next week you should:**
  - Revisit today's materials and start to initiate your own strategic planning. *Who do you need at the table with you?*
- **In the first three months following this presentation you should:**
  - Establish (or update) your organization's Vision and Mission.
  - Work with key stakeholders to build (or refresh) your strategic plan.
- **Within six months you should:**
  - Roll out your cybersecurity strategic plan, with stakeholder alignment and key, near-term initiatives underway.

RSAC 2025 Conference

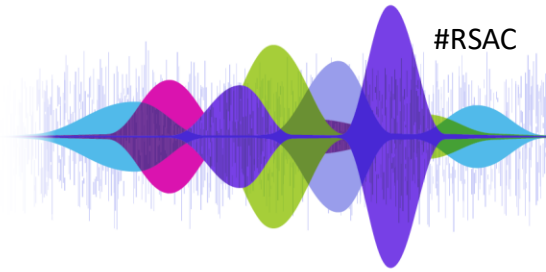
Many Voices.
One Community.

Thank you!

For more information, contact us at:

rachel@qubricsecurity.com

cora@qubricsecurity.com



END OF PRESENTATION

RSAC 2025 Conference

HANDOUTS

TO BE PRINTED FOR BREAKOUT SESSIONS

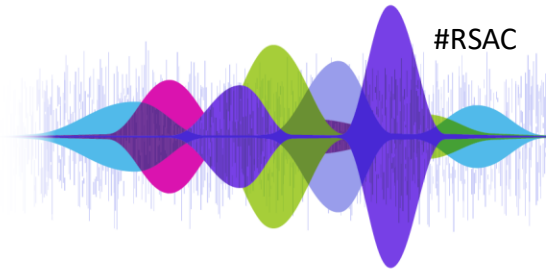
Many Voices.
One Community.

SecureBank Company Cybersecurity Challenges

- Bank is expanding its digital services to capture a larger share of the mobile banking market.
- It has recently upgraded its mobile app to allow easier access to services like peer-to-peer payments, loan applications, and mobile deposits.
- SecureBank handles a wide variety of sensitive financial data, such as account balances, credit scores, and transaction histories.
- While the company has implemented some multi-factor authentication (MFA) protocols for online services, there are concerns about employees' lack of proper security training.
- The bank's IT infrastructure is a mix of on-premises and cloud-based systems, but the cloud services are not fully integrated, leading to potential gaps in visibility and security.
- Recently, there's been a rise in phishing and social engineering attacks targeting employees and customers, leading to minor data leaks.
- As SecureBank strategically expands their services, they are increasing reliance on third parties.

SecureBank's Vision and Mission Statements

	SecureBank	SecureBank's Cybersecurity Team
Vision	To be the bank of choice for individuals and businesses, offering trusted financial services and innovative solutions.	**To be the cornerstone of SecureBank's innovation and customer trust.**
Mission	To deliver straightforward, reliable financial services that meet our customers' needs with a focus on trust, service, and growth.	**To deliver a secure and trusted banking experience by safeguarding our digital ecosystem and empowering business innovation.**



Breakout #1: Current State Assessment

Current State Assessment Worksheet

Step 1: Identify and Review Key Inputs

Category	Consideration
Business Goals	Digital banking expansion, secure mobile services, customer trust
Regulatory Requirements	GDPR (for European customers), PCI DSS (for payment security)
Threats	Phishing/social engineering, DDoS, third-party risk

Step 2: Discuss as a team and select one cybersecurity domain you will focus on (circle one):

Identity and Access Management

Security Training and Awareness

Cloud Security

Third Party Risk Management

Current State: Identity and Access Management

Area	Current State
People	• IT Operations handles user provisioning/deprovisioning manually. • Employees and contractors (20% of workforce) have different access requirements but are treated similarly. • HR and IT have a defined process for managing employee offboarding.
Process	• Managers complete employee end-user access reviews annually. • There is no centralized identity governance process; different identity types are managed independently. • User access is granted solely based on requests and manager approvals, and there is no formal structure to ensure consistency across similar job functions. • There are inactive accounts that still have access to applications and systems.
Policy	• Access management policies exist. • Password policies require complexity but allow password reuse. • There is no formal enforcement of least privilege access.
Technology	• Active Directory (AD) is used for user authentication. • Multi-factor authentication (MFA) is in place for some high-risk applications. • There is no privileged access management (PAM) solution. • Single sign-on (SSO) is used for some applications.

Current State: Cloud Security

Area	Current State
People	• The IT team is responsible for cloud security. • Business units often procure and set up their own cloud services (mostly SaaS). • Plan to send SOC Managers and Analysts to cloud training.
Process	• SOC Analysts manually review cloud security alerts and volume is steadily increasing. • Data classification and protection requirements are not consistently applied in cloud environments. • Cloud service providers (CSPs) are treated like any other vendor for third party risk management.
Policy	• No formal cloud security policy. Internal policies and standards have not been updated for cloud. • Access control policies differ across cloud and on-prem systems. • Employees are allowed to access and use personal cloud storage solutions.
Technology	• Security tools and controls are not standardized across cloud environments. • Enabled CSP-default security configuration and policies. • Logging and monitoring are not explicitly required for all cloud services. • No automated posture management or threat detection for cloud workloads.

Current State: Security Training and Awareness

Area	Current State
People	• HR is responsible for developing security training and it is a fairly generic module.
Process	• All new hires receive the same training regardless of role. • Employees are encouraged to report security incidents, but there is no formal process or tracking of reported cases. • HR captures tracks on-time training completion across the employee population; however, there are no metrics to measure training effectiveness, so it's unclear if employees are improving.
Policy	• Security training is required as part of new hire onboarding and once a year thereafter. • Security training for contractors is not enforced. Third parties are asked as part of vendor security reviews if they have a security awareness program. • Employees can repeatedly fail phishing tests without any consequences.
Technology	• LMS (Learning Management System) exists, but security training is a basic ‘click-through’ course. • Just-in-time training mechanisms (e.g., pop-up warnings before clicking suspicious links) have been discussed but were never implemented. • Phishing tests are administered manually and conducted on an ad hoc basis.

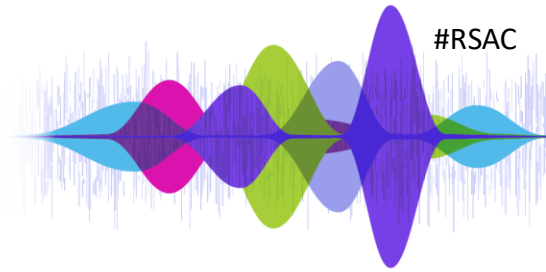
Current State: Third Party Risk Management

Area	Current State
People	• Procurement manages vendor contracts. • Vendor security reviews are conducted by the Legal team through self-assessment questionnaires. • Responsibility of third-party risk management is shared across multiple departments.
Process	• All vendors are treated the same regardless of risk level. • Vendor security reviews only occur at the time of onboarding. • No process exists for terminating vendor access when contracts end.
Policy	• There is a formal third-party risk policy that applies to all vendors. • No contractual requirement for vendors to notify SecureBank of security incidents affecting their data. • Incident response coordination with vendors is not clearly defined.
Technology	• Vendor risk assessments are conducted via spreadsheets and exchanged through email. • Third-party integrations rely on APIs. • Secure file-sharing solutions exist but are not mandated for vendor communications.

Current State Assessment Worksheet

Step 3: Analyze SecureBank's posture in the selected cybersecurity domain (refer to current state overview slides).

Current State	Gaps/Opportunities
People:	
Process:	
Policy:	
Technology:	



Breakout #2: Risk Assessment

Risk Assessment Worksheet

Step 1: Assign a Probability Score (*How likely is this risk to occur given existing controls?*)

Score	Description
1 – Low	Strong controls exist, and no incidents or warning signs suggest this is a realistic concern.
2 – Medium	Some gaps in controls exist, and past incidents or warning signs indicate this could happen.
3 – High	The issue is actively occurring or highly probable due to weak or failing controls.

Step 2: Assign an Impact Score (*What would happen if this risk occurs?*)

Score	Description
1 – Low	Minimal disruption, minor financial loss, or easily contained.
2 – Medium	Some disruption, moderate financial or reputational damage.
3 – High	Severe impact, major financial loss, and/or regulatory consequences.

Note: Organizations should customize the risk matrix based on their needs. For example, quantification of sub-categories - such as assigning percentage intervals to probability and quantifying financial impact - can help drive more consistent risk ratings and provide further context to relative risk.

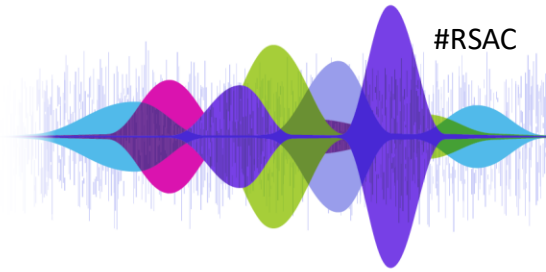
Risk Assessment Worksheet

Step 3: Select 2-3 gaps to risk assess. Calculate the risk score of each gap by multiplying probability by impact.

No.	Gap	Probability (1 – 3)	Impact (1 – 3)	Score (Prob x Impact)
1				
2				
3				

Step 4: Prioritize Based on Risk Score (Probability x Impact):

- **6-9 (High Risk)** → Immediate priority, needs urgent action
- **3-4 (Medium Risk)** → Needs attention but not urgent
- **1-2 (Low Risk)** → Low priority, address when resources allow



Breakout #3: Target State Planning

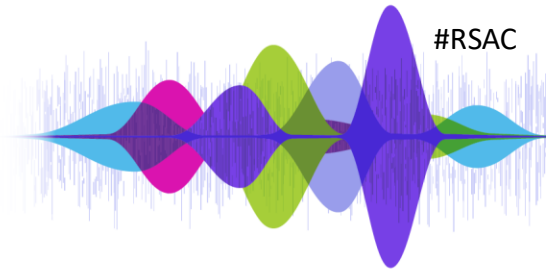
Target State Planning Worksheet

Step 1: Define a target state, strategic objective for SecureBank.

Strategic Objective:

Step 2: Specify goals with near-, mid-, and long-term milestones. Define supporting projects with estimated resource needs.

Near-Term	Mid-Term	Long-Term
Goal:	*Goal:*	*Goal:*
Projects | Resource Needs (S, M, L):	*Projects | Resource Needs (S, M, L):*	*Projects | Resource Needs (S, M, L):*



END OF HANDOUTS